Release Notes

hp StorageWorks Data Replication Manager HSG80 ACS Version 8.7P

Product Version: ACS Version 8.7P

Fifth Edition (March 2004)

Part Number: AA-RPJ2E-TE

This document provides information for HP StorageWorks Data Replication Manager with HSG80 Array Controller Software Version 8.7P that is not covered elsewhere in user documentation. Individuals responsible for configuring, installing, and using the Data Replication Manager solution should refer to this document for last-minute content.

For the latest version of these Release Notes and other Data Replication Manager documentation, access the website at http://h18000.www1.hp.com/products/sanworks/drm/index.html. Click the **technical documentation** link and the technical support page is displayed. Click **manuals (guides, supplements, addendums, etc)** for a listing of related documentation.

invent

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Data Replication Manager HSG80 ACS Version 8.7P Release Notes
Fifth Edition (March 2004)
Part Number: AA-RPJ2E-TE

Release Notes Contents

These release notes cover the following major topics:

Intended Audience

This document is intended for customers who purchased or upgraded to the HP StorageWorks Data Replication Manager (DRM) HGS80 Array Controller Software (ACS) Version 8.7P, and for HP authorized service providers responsible for installing, configuring, and maintaining DRM systems.

Related documentation

The following documents provide helpful information for running your DRM solution:

- *HP StorageWorks Data Replication Manager HSG80 Version 8.7P Configuration Guide*, part number AA-RPHZF-TE
- *HP StorageWorks Data Replication Manager HSG80 Version 8.7P Failover/Failback Procedures Guide*, part number AA-RPJ0E-TE
- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Scripting User Guide*, part number EK-DRMSC-OA. E01
- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Design Guide Reference Guide*, part number AA-RQ78C-TE
- *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide*, part number AA-RU5CE-TE
- *HP StorageWorks SAN Design Reference Guide*, part number AA-RMPNL-TE

What’s New

The following sections summarize the major features, enhancements, and requirements of using ACS Version 8.7P with DRM.

SAN Extension Products

Refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide* for details on supported Fibre Channel over Internet Protocol products. All WDM products are permitted with Continuous Access EVA and Data Replication Manager.

Controller Firmware Upgrade Path

HP strongly recommends that the minimum version of DRM for new installations or upgrades be ACS v8.7-3P. This version should be obtained from a direct install and not by overlaying patches on earlier versions of 8.7P. For information on obtaining the appropriate ACS v8.7-3P PCMCIA card, contact your HP service center.

The rolling upgrade is documented in the *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Configuration Guide*. The procedure is designed to allow an array controller software upgrade without the need for a server reboot. However, you must ensure that all the latest drivers, and if applicable, the latest release of Secure Path are installed prior to this upgrade. Installing the latest drivers may require the server to be rebooted. Information on the latest supported drivers and Secure Path can be found in Table 1.

Operating System and Fibre Channel Switch Support

Support has been added for newer operating systems and switch firmware. Table 1 lists the minimum hardware and software versions of items supported by those operating systems compatible with Data Replication Manager running ACS v8.7P and subsequent updates. Operating systems are listed by vendor in the left column. Each item in the same row, and listed to the right, is supported by that operating system.

To use this table, select an operating system and operating system version, then move to the right and select a Fibre Channel Adapter (FCA). Supported FCA firmware is located further to the right, followed by the driver and Secure Path versions for the FCA. In the last column is a brief statement about cluster support for that operating system and version.

Table 2 lists supported switches for the HSG80 controller with their approved version of firmware when used for DRM. Be aware that a 2 Gb/sec switch is constrained by the HSG80 controller to 1 Gb/sec.

Table 1: Operating System Support Matrix

Operating System	OS Version	FCA	Adapter Firmware	Adapter Driver	Secure Path	Clustering
HP HP-UX	11.0 (32-bit with 0303 patch bundle) 11.11 (32-bit with 0603 patch bundle)	A5158A 1Gb PCI A6685A 1Gb HSC A6795A 2Gb PCI	Native	Native	3.0aSP1 or 3.0bSP1	ServiceGuard v11.14 Max: 4 nodes
HP OpenVMS	7.2-2 with VMS722_FIBRE_SCSI-V0400 7.3 with VMS73_FIBRE_SCSI-V0500 7.3-1 with VMS731_FIBRE_SCSI-V0100	LP8000 or LP9002 (FCA2354)	3.81a4, 3.82a1, 3.91a1, or 3.92a0	Native	Native	VMSCluster Max: 96 nodes
		LP9802 (FCA2384)	1.00x8 or 1.81a1			
HP Tru64 UNIX	5.1a BL22 PK4 5.1b BL1 PK1	LP8000 or LP9002 (FCA2354)	3.81a4, 3.82a1, 3.91a1, or 3.92a0	Native	Native	TruClusters Max: 8 nodes
		LP9802 (FCA2384)	1.00x8 or 1.81a1			
IBM-AIX	4.3.3, 5.1	Cambex 1Gb PCI (1000F)	2.01.38	1.5.20.2	2.0c	v5.1 supports HACMP v4.5
		Cambex 2Gb PCI (2000F)		1.5.23.2	2.0d	

Table 1: Operating System Support Matrix (Continued)

Operating System	OS Version	FCA	Adapter Firmware	Adapter Driver	Secure Path	Clustering
Microsoft Windows NT (Intel) Windows 2000 (32-bit)	4.0 SP6a 5.0 SP2, SP3, SP4	LP8000 (KGPSA-CB) LP952 (FCA2101)	3.82a1 BIOS 1.60a5	4.81a9	4.0c	NT - 2 nodes Windows 2000 Server - none Windows 2000 Advanced Server - MSCS v1.1 & Oracle 9iRAC; Max: 2 nodes Windows Server 2003, Enterprise edition - MSCS & Oracle 9iRAC; Max: 4 nodes
			3.82a1 BIOS1.61a2	4.82a14		
			3.91a1 BIOS1.63a1	4.82a16		
		LP9002DC (FCA2355)	3.82a1 BIOS 1.61a2	4.82a9		
				4.82a14		
			3.91a1 BIOS 1.63a1	4.82a16		
		QLA2340 (FCA2214) or BL20P Mezzanine card (not supported on NT)	1.34	8.2.0.72		
		QLA2342 (FCA2214DC) or BL20P Mezzanine card (not supported on NT)	1.34	8.2.0.72		
		LP982 (FCA2408) (not supported on NT)	1.01a2	4.82a16		
		LP9802 (FCA2404) and LP9802DC (FCA2404DC) (neither supported on NT	1.01a2	4.82a16		
Novell NetWare	5.1 SP6, 6.0 SP3	QLA 2340 (FCA2210)	1.29	6.50.z	3.0c with SP1	N5.1 supports NCS V1.01 V6.0 supports NCS v1.06, Max: 6 nodes
Sun Solaris	2.6, 7, 8[1]	JNI FCI-1063 (32-bit PCI)	3.0.3	2.5.9-03	3.0c with SP1	Veritas Cluster Services v2.0 or v3.5; Max 16 nodes Sun Clusters v2.2; Max: 16 nodes
	2.6, 7, 8	SWSA4-SB 1 Gb 32-bit SBUS	13.3.7			
		JNI FC64-1063 (64-bit Sbus)				
	2.6, 7, 8, 9	QLA2202 Sbus 1Gb (FCA2257S)	FC 1.18.3, firmware comes with driver	4.11		
		QLA2310 Sbus 2Gb (FCA2257P)	FC 1.18.5, firmware comes with driver			
	8 or 9 Build 2	QLA2202 cPCI 1Gb (FCA2257C)	FC 1.18.5, firmware comes with driver			

[1] If used with 2 Gbps B-series switches, you must use the latest switch firmware (v2.2.1c, v3.1.1c, or 4.1.2b at time of publication).

Table 2: Supported Switches for the HSG80

Fibre Channel Switch	DRM Supported Switch Firmware
B-Series	
HP StorageWorks SAN Switch 8, 16, 8-EL, and 16-EL (1 Gb)	2.6.2 preferred 2.6.1c optional
HP StorageWorks SAN Switch 2/8, 2/16, 2/8-EL, and 2/16-EL (2 Gb)	3.2 preferred 3.1.1c optional
HP StorageWorks SAN Switch Integrated/32 and Integrated/64	2.6.2 preferred 2.6.1c optional
HP StorageWorks SAN Switch 2/32	4.2 preferred 4.1.2b optional
C-Series	
Cisco MDS9120, MDS9140, MDS9216, MDS9506, and MDS9509	1.2.1b
M-Series	
HP StorageWorks Edge Switch 2/24	5.02.00-13
HP StorageWorks Edge Switch 2/16 and 2/32	5.02.00-13
HP StorageWorks Core Switch 2/64	4.2 preferred 4.1.2b optional
HP StorageWorks Director 2/64	5.02.00-13
HP StorageWorks Director 2/140	5.02.00-13

Common Platform Issues

Performance Considerations—Adding Target Unit Back to Remote Copy Sets

Each remote copy set is forced into a full normalization when you add back the target unit using the following command:

```
SET RemoteCopySetName ADD = TargetRemoteCopyName\UnitName
```

```
Example: set rcs1 add = buildngA\d1
```

In some cases this normalization has an impact on data replication performance and therefore should not be performed during periods of high I/O activity at the target site. You may wish to stagger the normalization of each remote copy set to minimize the performance impact.

Performance Considerations—Full Copy Operation

During full copy operations, host I/O performance is moderately reduced, and the length of time required for the copy operation is longer than that for a merge operation.

Performance Considerations—Write History Log Merge

During Write History Log merge, host I/O performance is drastically reduced due to the high priority given to the merge operation. The length of time required for the merge operation is affected by host I/O, as new I/O is added to the end of the Write History Log, while the oldest is pulled from the beginning of the log.

SWCC and OpenView Management Appliance Limitations

The HSG80 controller does not distinguish between commands issued from in-band command tools (SWCC, Command Scripter, or the HP OpenView Storage Management Appliance) and commands issued out of band through the serial port. Serial port commands should be performed only when the customer has restricted commanding from other sources. Special care must be taken with the Storage Management Appliance (SMA), as it periodically issues polling commands that can interrupt serial port communications. If you will be using the serial port on the HSG80 controller, remove the SMA from the fabric or use switch zoning to isolate the SMA from the array in which controllers are commanded through a serial port.

Using Switch Zoning to Prevent Crashes When Using VTDPY Host Display

The HSG80 controller may crash when using the Display Host functionality in VTDPY. If more than 21 connections are displayed (the equivalent of one page), the controller will crash with a last fail code of 01932588 (cache data allocation parity error). HP recommends that you use switch zoning to limit the number of connections visible to the controller. For more information about switch zoning, refer to the *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Configuration Guide*.

Invalid VTDPY Percentages

During the transition time between site failover and site failback, the log, merge, and copy percentages on the original initiator displayed by VTDPY are not valid. Disregard these percentages.

Using Switch Zoning to Prevent Crashes When the 96-Connection Limit Is Exceeded

The HSG80 controller may crash if more than 96 connections exist on the fabric. HP suggests that you use switch zoning to limit the number of connections visible to a single HSG80 controller. For more information about switch zoning, refer to the *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Configuration Guide*.

I/O Pause During Fabric Reconfiguration

During a fabric reconfiguration, you will notice a brief pause in I/O functions on all servers connected to the fabric. This brief cessation of read/write operations is normal. A fabric reconfiguration can be caused by switches starting up or shutting down, and by the physical plugging or unplugging of fiber cables.

Controller Saturation

High usage of many remote copy set and nonremote copy set LUNs has a serious impact on the performance of the remote copy set LUNs, causing controller saturation and possibly starving a full copy operation.

A saturated controller condition begins approximately when idle time falls to 25% or less when viewed through VTDPY. When this occurs, you may see Aborted Command errors through the Command Line Interface (CLI).

To prevent controller saturation:

- Avoid placing multiple heavy-use loads on the controllers.
- Use the VTDPY screen to monitor controller idle time percentage. Adjust load to maintain an idle time of 25% or greater.

RAID 5 Remote Copy Set Target Drop

Under the following combined conditions, RAID 5 remote copy set targets may be dropped:

- No write history log disk is configured, and
- Host I/O is accessing the initiator remote copy set LUNs.

When both target controllers are shut down, a full copy operation is triggered. When the target controllers are restarted, they will begin a 3-minute memory diagnostic.

While the memory diagnostics are running, the full copy I/O to RAID 5 target LUNs is stalled. Therefore, after approximately 2 minutes, a timeout occurs and the target LUNs are dropped from the remote copy set. This target drop problem occurs only on RAID 5 remote copy set LUNs.

- To prevent target LUN drop:
  1. Set port_2_topology on both initiator controllers to *offline* before target controllers are booted and powered on.
  2. Wait five minutes after target controllers are restarted to allow for memory diagnostics to complete.
  3. Set port_2_topology on the initiator controllers back to *fabric*.

- If the target LUNs are dropped:
  1. Wait five minutes to allow for the target controller memory diagnostics to complete.
  2. Add the targets back into the remote copy sets.

  The full copy operation begins.

Required Delay Time Before Failback

Be careful that you do not start a site failover or site failback process too soon. You must wait a minimum of 15 minutes from the completion of a site failover process to begin a site failback procedure. You must also wait a minimum of 15 minutes from the completion of a site failback process to begin a site failover procedure.

Removing Targets from the Proper Controller

The target of a remote copy set should be removed by the controller to which it is online. A problem occurs if both fabric intersite links are not functioning and you remove the target of a remote copy set that is part of an association set with a write history log. If you try to remove the target from the controller that the remote copy set is not online to, and then issue the CLI command `SHOW REMOTE COPY SET FULL`, the target state will indicate LUN D0 is copying 0% complete. The actual indication of the target state should be "No targets."

Example:

```
Name                                         Uses             Used by
---------------------------------------------------------------------------
RCS1         remote copy                    D1               AS1
        Reported LUN ID: 6000-1FE1-0007-9DD0-0009-0510-3907-000E
        Switches:
          OPERATION_MODE  = SYNCHRONOUS
          ERROR_MODE      = NORMAL
          FAILOVER_MODE   = MANUAL
          OUTSTANDING_IOS = 20
        Initiator (BUILDNGA\D1) state:
          ONLINE to the other controller
        Target state:
          \D0             is COPYING                0% complete
```

Another problem occurs when you try to add the target back in. You will see the %EVL error message: "Too many targets have been specified in this set." You cannot add a target if you are in a normal production mode or if you are in a failed-over condition. You must first issue the CLI command to delete the remote copy set, and then issue the CLI command to add the remote copy set back in. Deleting and then re-adding the remote copy set will force normalization.

If your intersite links will be down for an extended period of time after a failover, HP recommends that you delete your associations sets and then remove your remote copy sets to the target controller. This may require a remapping of your host to LUN connections with some operating systems. Run the initiator controller in standalone mode until your intersite links are re-established.

Startup of Only One Fabric at a Time

When an event occurs that causes a fabric reconfiguration (for example, a scheduled or unscheduled outage of an intersite link, addition or removal of a switch or switch-to-switch link, and so on), allow all of the Fibre Channel switches in that fabric to reconfigure before you reconfigure the second fabric.

Intermittent Double Normalization After a Full Failback or Failback to New Hardware Procedure

After you have performed a full failback or failback to new hardware, a second normalization (from the initiator to target) can occur. This double normalization happens after the point in the failback procedure where you add the target and normalize your storage sets (from the target to initiator).

The only effect of this extra normalization is to add the additional controller overhead of doing a full copy—it causes no data corruption. When normalization is complete, you can proceed with the failback and add the load at the appropriate point in the procedure.

Command Scripter Communication Loss Due to SCSI Error

If Command Scripter v1.0A has a loss of communication while a script is running, it will cause the script to abort. You must then put the controllers in a known state by issuing the appropriate CLI commands from the controllers. You can examine the .log files in the $CLONE_HOME/log directory to determine which commands were executed before communication was lost.

If the communication failure is due to a SCSI error, then the loss of connection is only momentary. You can verify that the connection is re-established by issuing the following command from the host:

```
cmdscript -f <device Name> "show this"
```

However, if this command continuously gives a communication failure error, a hardware failure or configuration error is indicated. Troubleshoot the loss of connection for causes such as broken links, failed devices, controller configuration, and so on.

Waiting for Write History Logging Disks

After clearing invalid cache and lost data, remote copy set processing will halt. When you issue the CLI command `SHOW REMOTE_COPY_SETS FULL`, you may see the following error message:

```
Waiting for write history logging disks to become ready.
```

Restart the controller to clear this condition.

Association Sets

Association sets can contain up to 12 remote copy sets. However, because all remote copy sets within an association set are moved between controllers as a group, all remote copy sets within an association set must be accessed by the same server.

For instance, 6 remote copy sets (one association set) could be accessed by one server and 6 remote copy sets (another association set) by the other.

Platform-Specific Issues

HP HP-UX

Failure to Mount File System after Failover or Failback

If you are unable to mount a previously configured file system after a failover or failback, run File System Check on the logical volume and retry the mount.

```
Example: FSCK -O full /dev/vg0#/lvol#
```

Configuring Host Server Remote Copy Sets

Remote copy sets (RCSs) at the target site will acquire the world wide name of their RCSs at the initiator site when a failover occurs. HP recommends that you not configure the RCS on the HP-UX host servers at the target site until after a failover.

HP OpenVMS

Additional Software Requirements

Remedial kits that you may require are available at:

ftp://ftp.itrc.hp.com/openvms_patches/alpha

HP Tru64 UNIX

Prevent Possible Data Corruption

If during the failover procedure you are unable to stop all applications and dismount all units that are part of a remote copy set, you must reboot hosts prior to failback. Doing this prevents possible data corruption caused by writing stale data from host cache to the units after failback.

Note: Extreme care must be used when creating and managing remote copy sets on an ATM link. If these links are overstressed (for example, an excessive number of remote copy sets created for a given environment), unexpected behavior may result, such as loss of remote copy sets and link failures.

Accessing Special Device Files During Fabric Failover

HP recommends that no attempt be made to access the special device files during a fabric failover. Running any commands against the block or raw devices in /dev/disk or /dev/rdisk is highly discouraged. In rare instances, running the `FILE` command against raw or block devices during a fabric failover has prevented the surviving path from coming online following failure of the original path.

IBM AIX

Increased LUN Support

Beginning with Secure Path Version 1.5.19.1 for the Cambex drivers, the maximum number of LUNs supported increased from 16 to 32.

Microsoft Windows 2000

Auto Failback

The Secure Path for Windows 2000 Auto Failback feature is not currently supported in a Data Replication Manager configuration. Disable this feature by starting Secure Path Manager, then selecting **Properties** > **Autofailback** > **Disable**.

Booting Windows 2000 Servers Over the Fabric

Any of the Windows servers can be booted from a LUN on an HSG80 controller, including a LUN that is part of a remote copy set. Instructions for configuring servers and booting Windows 2000 are available for download from the Web at:

http://h18000.www1.hp.com/support/storage/open_vendor/support/RAIDarray/boot_support_external_web.html

Two problem situations could arise when booting over the fabric:

- If the boot LUN is online to a controller that the server cannot access, the server will be unable to boot. This condition could occur if the link between the server and the fabric is broken. At this stage of booting, the server cannot move the LUN between controllers. The LUN must be manually moved to the other controller by issuing the following CLI commands:

  ```
  SET UNIT_NUMBER PREFERRED=OTHER
  SET UNIT_NUMBER NORUN
  SET UNIT_NUMBER RUN
  ```

- When an intersite link with high latency (such as ATM) is used, the server may take a long time to boot and may be slow to respond during normal operation. This is normal behavior for the server. It is caused by the time required to replicate the boot disk across a very long distance.

Check Status

If a target controller or switch becomes inoperative and the Windows 2000 host is rebooted, Secure Path Manager will not report that you have lost multipath capability.

If you attempt to move a LUN to the inoperative path, a warning message appears, indicating that you should check the Application Event Log for details. This may be an indication that you have lost multipath capability.

Check the status of links, target switches, and target controllers.

HSG80 Controller Soft Shutdown/Restart

When the `SHUTDOWN THIS` or `SHUTDOWN OTHER` command is executed from the CLI, the controller will shut down, forcing the LUNs to change paths. Secure Path will immediately fail the LUNs over to the remaining path, but the original path may not be marked as failed for several minutes.

Similarly, when the `RESTART THIS` or `RESTART OTHER` command is executed from the CLI, the controller will restart, forcing the LUNs to change paths. Secure Path will immediately fail the LUNs over to the remaining path, but the original path will never be marked as failed. The icon for the failed LUN will be marked with a yellow triangle with an exclamation point inside. The controller will finish restarting and return to normal operation without notification.

The following procedure can be used to check whether a system is in this state:

1. Select one of the units in Secure Path Manager.
2. Click the path marked **Available** in the right-hand pane*,* and then right-click it to bring up the menu.
3. Select **Verify Path** from the menu that appears.

If the verify fails, the path is not available. The path becomes available again after the controller is booted.

Component failures and other real failure scenarios cause paths in Secure Path to be correctly marked as failed.

LUNs Lettered Incorrectly

When LUNs are moved between hosts (such as during a site failover or a site failback), it is possible that the LUNs may become “out of letter order.”

To prevent the “out of letter order” status, follow the steps below:

1. Before booting the Windows 2000 host, make sure all LUNs are failed over to one HSG80 path. From the HSG80 CLI prompt, issue the following command:

   ```
   Restart Other_Controller
   ```

2. Reboot the Windows 2000 host.
3. Use Disk Manager to assign the correct drive letter so that the disks now match the units on the controller.
4. Once Windows 2000 sees the disks ordered properly, use Secure Path Manager to move the units to the correct path.

Changing Host Connection Unit Offsets

If the UNIT_OFFSET of a connection is changed, the host must be rebooted to recognize the change. The host will continue to operate using the offset that was previously in effect until it is rebooted. For example, if a host connection has a unit offset of zero, it will be able to access only units D0 through D7. If the offset is changed to 8, the host will still be able to access units D0 through D7 until it is rebooted. After reboot, it will be able to access only units D8 through D15.

Windows 2000 Plug and Play Manager Generates Numerous Pop-up Windows

Each time a LUN is dismounted ungracefully (for example a fabric failure), Windows 2000 displays a pop-up window that warns of “Unsafe removal of device.” This window can be cleared by simply clicking **OK**. The window itself is harmless, but additional dismounts cause more pop-up windows to appear. These windows can stack up on the desktop and consume memory to the point that the system crashes. However, several hundred dismounts and associated pop-up messages are required before a system crash is probable.

Windows Using Large LUNs While in SCSI-2 Mode

DRM supports Windows 2000 hosts accessing large LUNs above D7 without offsets via Secure Path. However, all hosts using large LUNs on a controller in SCSI-2 mode must create a dummy LUN 0 and give access to this LUN. HP also recommends that this phantom LUN be set to “no write” access. Refer to the *HP StorageWorks Secure Path for Windows Installation and Reference Guide* for additional information.

Association Sets

In a Windows 2000 cluster configuration, all remote copy sets within an association set must be placed in one cluster resource group.

Microsoft Windows NT

Auto Failback

The Secure Path for Windows NT Auto Failback feature is not currently supported in a Data Replication Manager configuration. Disable this feature by starting Secure Path Manager, and then selecting **Properties** > **Autofailback** > **Disable**.

LUNs Lettered Incorrectly

When LUNs are moved between hosts (such as during a site failover or a site failback), the LUNs may become “out of letter order.”

To prevent the “out of letter order” status, follow the steps below:

1. Before booting the Windows NT-X86 host, make sure all LUNs are failed over to one HSG80 path. From the HSG80 CLI prompt, issue the following command:

   ```
   Restart Other_Controller
   ```

2. Reboot the Windows NT-X86 host.
3. Use Disk Administrator to assign the correct drive letter so that the disks will now match the units on the controller.
4. Once Windows NT sees the disks ordered properly, use Secure Path Manager to move the units to the correct path.

Windows Using Large LUNs While in SCSI-2 Mode

DRM supports Windows NT hosts accessing large LUNs above D7 without offsets via Secure Path. However, all hosts using large LUNs on a controller in SCSI-2 mode must create a dummy LUN 0 and give access to this LUN. HP also recommends that this phantom LUN be set to “no write” access. Refer to the *HP StorageWorks Secure Path for Windows Installation and Reference Guide* for additional information.

Association Sets

In a Windows NT- X86 cluster configuration, all remote copy sets within an association set must be placed in one cluster resource group.

Novell NetWare

NetWare Cluster Services (NWCS)

NWCS v1.01 SP1 for NetWare 5.1 and NWCS v1.6 for NetWare 6 are supported at the initiator and target sites. Stretch clusters are not supported at this time. A stretch cluster is defined as having a NetWare Cluster using NWCS with cluster members located at both the DRM initiator and target sites. NWCS supports both remote copy set and nonremote copy set LUNs.

Planned Failover/Failback with NWCS

When preparing the initiator and target sites for a planned failover/failback, use caution when removing access to the LUNs at the initiator site. Removing access to the split brain detector (SBD) partition, as well as the cluster volumes, without first bringing down the cluster will result in server abends. To avoid cluster members abending, issue the following command at the system console:

```
CLUSTER DOWN
```

You can also run `ULDNCS.NCF` at the system console for each cluster member to unload cluster services completely.

NetWare 6 Storage Planning Considerations

If you plan on using Novell Storage Services (NSS) logical volumes in a DRM configuration, you should be aware that the nature of Novell's Distributed File Services (DFS) allows you to span an NSS volume across multiple hard disk partitions. This is not desirable in a DRM configuration. Instead, you should maintain a one-to-one relationship among LUNs, remote copy sets, NSS partitions, NSS pools, and NSS logical volumes.

Additional Instructions for Failover/Failback

When NetWare volumes are created at the initiator site, they are inserted into the Novell Directory Services (NDS) tree as servername_volumename (for example, SERVER1_VOL1). After a site failover, the replicated NetWare volumes are still available and can be mounted by any NetWare server at the target site, but the volumes will now take on the new server name (for example, SERVER2_VOL1). In addition, they will not be automatically inserted into NDS, and for traditional NetWare volumes only, they will not maintain the file system permissions established at the initiator site. You MUST perform the following steps the first time failed-over volumes are mounted at the target site:

Traditional NetWare Volumes

After failing over to the target site and mounting the NetWare volumes:

1. Type `nwconfig` from the file server console.
2. Select **Directory Options**.
3. Select **Upgrade Mounted Volumes into the Directory**, and supply an administrator-equivalent userid and password.

4. Access a Windows workstation (or the file server's graphical console) and use the *ConsoleOne* utility to establish the desired file system permissions for the newly inserted volumes.

NSS Logical Volumes

After failing over to the target site and mounting the NSS logical volumes:

1. Run *ConsoleOne* from a Windows workstation or the file server's graphical console.
2. Select **Disk Management > NSS Pools** from the **Tools** menu.
3. Select the correct **NDS Tree**, **NDS Context**, and **Server** when prompted.
4. Ensure that the **Media** tab is highlighted and **NSS Pools** is displayed. Click the correct **NSS Pool** from the list on the left to highlight the pool, and then click the **Update NDS** button.
5. Click the **Media** tab and then **NSS Logical Volumes**.
6. Click the correct **NSS Logical Volume** from the list on the left to highlight the volume, and then click the **Update NDS** button.

Note: You must perform steps 4 through 6 above for each NSS Pool/Volume pair you fail over from the initiator site.

After the above procedures are accomplished, they will not have to be performed again as long as the volumes are always mounted on the same target file server after a failover.

Upon failback to the initiator site, any new files or directories created at the target site will need to have permissions reestablished using the ConsoleOne utility (for traditional NetWare volumes only). When performing subsequent failovers, it is not necessary to insert the volumes into the NDS tree—they will already be there. Simply make sure that the necessary permissions are granted using ConsoleOne if any new files or directories have been created at the initiator site (for traditional NetWare volumes only).

CPU Hog Abends

If you experience CPU Hog Timeout server abends, you may have to adjust the CPU Hog Timeout amount (using *MONITOR.NLM* under the menu parameter Server Parameters, Miscellaneous) to a lower amount or 0 seconds (disabled).

Auto Failback

Auto Failback is supported using Secure Path for NetWare. Failures involving the target site (extended intersite link failures, target switch failures, target controller failures) cause Secure Path to fail LUNs to their alternate paths. However, Auto Failback to the preferred path may not occur after the link is restored. In these situations, use the Secure Path Manager (GUI) to manually move LUNs back to their preferred paths. Refer to the *HP StorageWorks Secure Path for Novell Netware Installation and Reference Guide* for additional details on performing this operation.

Partitioned LUNs

Novell servers cannot access partitions if another partition on the same physical disk (LUN) is accessed by another operating system. When this happens, the Novell server may lock up. To prevent lockup, remove any other operating systems accessing the partitions.

Maximum Number of Host Bus Adapters

The maximum number of host bus adapters supported by a Novell host is four. This is a limitation of Secure Path.

Sun Solaris

Memory Requirement

Sun Solaris requires at least 512 MB RAM per CPU when running ACS v8.7P. Edit the *etc/system* file to include the following line:

```
set lwp_default_stksize=0x8000
```